



## APPLICATION FOR U.S. PATENT TRANSMITTAL FORM

April 30, 1999  
 Box PATENT APPLICATION  
 Assistant Commissioner for Patents  
 Washington, D.C. 20231

Dear Sir:

EXPRESS MAILING label number EJ429165231US  
 Date of Deposit: April 30, 1999  
 I hereby certify that this paper is being deposited with the U.S.  
 Postal Service Express Mail Post Office to Addressee Service under  
 37 C.F.R. § 1.10 on the date shown above and is addressed to the  
 Assistant Commissioner of Patents, Washington D.C. 20231.

  
 Alan W. Lintel

Transmitted herewith for filing is the patent application of:

Inventor(s): Gu

For: Pseudo-Noise Sequence With Insertion Having Variant Length and Position

Enclosed are a patent application including 15 pages of specification, 4 sheets of informal drawings, and a Declaration and Power of Attorney, as well as an Assignment (with cover sheet) of the invention to TEXAS INSTRUMENTS INCORPORATED.

FEE CALCULATION					FEE
			Basic Fee		760
	Number		Extra	Rate	
Total Claims	19	20	0	18	0
Independent Claims	2	3	0	78	0
<b>TOTAL FEES</b>					<b>760</b>

Please charge deposit account No. 20-0668 in the amount of the Total Fees set forth above. The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to said deposit account. **A duplicate copy of this sheet is enclosed.**

All correspondence regarding this application may be directed to Applicants' attorney at the below listed telephone number and address.

Ronald O. Neerings  
 Texas Instruments Incorporated  
 P.O. Box 655474, M/S 3999  
 Dallas, Texas 75265  
 (972) 917-5299

Respectfully submitted,

  
 Alan W. Lintel  
 Reg. No. 32,478

**PSEUDO-NOISE SEQUENCE WITH  
INSERTION HAVING VARIANT  
LENGTH AND POSITION**

CROSS-REFERENCE TO RELATED APPLICATIONS

Not Applicable

STATEMENT OF FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not Applicable

**5 BACKGROUND OF THE INVENTION**

**1. TECHNICAL FIELD**

This invention relates in general to communications and, more particularly, to spread spectrum communications and data encryption.

**2. DESCRIPTION OF THE RELATED ART**

10 Spread spectrum communication devices have been used in military and commercial devices for many years. These devices use noise-like waves to spread (cover) the information bits so that transmission bandwidth is much wider than that required for simple point-to-point communication. DS-CDMA (Direct Spreading Code Division Multiple Access) is a form of spread spectrum which uses a conventional communication waveform and a pseudo-noise (PN) sequence to transmit information. The PN sequence is commonly generated 15 using a Linear Feedback Shift Register (LFSR).

In addition to its improved capacity and quality, spread spectrum techniques provide secure communications, since the receiver will generate the same PN sequence as the transmitter. While normal spread spectrum devices are very secure relative to other communication devices, it is possible to determine  
5 the polynomial being used to generate the pseudo-noise sequence, since there are a finite number of polynomials for a given sequence length. While third-party deciphering the pseudo-noise sequence may require significant computing power, it is possible that such resources may be available to decipher highly confidential communications.

10 Accordingly, a need has arisen for a method and apparatus for generating a PN sequence which is difficult to decipher.

## BRIEF SUMMARY OF THE INVENTION

In the present invention, a communication signal is encrypted using an augmented pseudo-noise sequence. The augmented pseudo-noise sequence is created by generating a plurality of pseudo-noise sequences and combining these 5 pseudo-noise sequences, or portions thereof. The data signal is encrypted using the augmented pseudo-noise sequence.

The present invention provides significant improvements over the prior art. Insertion of one or more segments of arbitrary length from other PN sequences in real time at respective arbitrary points in a PN sequence creates a 10 PN sequence which is almost impossible to decipher. For each period of the augmented PN sequence, the segment parameters and insertion points may change, further increasing the complexity in decrypting the PN sequence.

## BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

- 5       Figure 1 illustrates a general overview of an augmented PN sequence;
- Figure 2 illustrates a preferred embodiment of an augmented sequence which allows for an offset and describes the formation of the augmented sequence;
- 10      Figure 3 illustrates a schematic representation of a circuit for generating the augmented sequence of Figure 2;
- Figure 4 illustrates a schematic representation of an augmented sequence using multiple segments; and
- Figure 5 illustrates use of the augmented pseudo-noise sequence to encode a data signal.

## DETAILED DESCRIPTION OF THE INVENTION

The present invention is best understood in relation to Figures 1 - 5 of the drawings, like numerals being used for like elements of the various drawings.

Figure 1 illustrates a general overview of an augmented PN sequence 10 for use in spread spectrum devices, or any other device using a PN sequence, formed from two or more PN sequences, PN0 sequence 12 and PN1 sequence 14. The augmented PN sequence 10, PN0 sequence 12 and PN1 sequence 14 could be streams of real or complex numbers, depending upon the application. For example, in a QPSK DS-CDMA system, the augmented PN sequence 10, PN0 sequence 12, and PN1 sequence 14 would be sequences of complex numbers,  $\text{PN}(k)=\text{PN}(k)_I+j\text{PN}(k)_Q$ , where  $\text{PN}(k)_I$  and  $\text{PN}(k)_Q$  are one bit values. Many other systems use sequences of real numbers.

A segment 16 of the PN1 sequence 14, which may be all or part of the PN1 sequence, is inserted into the PN0 sequence 12 at an arbitrary position INS\_POS of the augmented PN sequence. Segment 16 has arbitrary length SEG\_LTH.

In operation, the augmented PN sequence 10 can be used by a data scrambling device in place of the normal, unaugmented PN sequence. Because the augmented PN sequence includes insertion of a second sequence of arbitrary length at an arbitrary position in the augmented PN sequence, determining the polynomial would be exceeding difficult, even using supercomputers.

It should be noted that while the embodiment of Figure 1 illustrates an augmented PN sequence wherein a single segment 16 is inserted into another PN sequence, multiple segments from multiple PN sequences could be inserted into the pseudo-noise sequence, making it even more difficult to decrypt. Further, the starting and ending points of the segment(s) and the insertion point(s) can be modified as often as every period of the augmented PN sequence to further increase complexity.

Figure 2 illustrates a preferred embodiment which allows for an offset and describes the formation of the augmented sequence in greater detail. The offset allows greater flexibility for synchronization within the system. Figure 2 illustrates the Augmented PN sequence 10, PN0 sequence 12, PN1 sequence 14, relative to a reference clock (REF\_CT) 20. The reference clock 20 has the same period (AUG\_PRD) as the augmented PN sequence 10. OFFSET defines the shift between the starting point (the first word, where a "word" could be a one bit value for a PN sequence of real values or a two bit value for a PN sequence of complex values) of the augmented PN sequence 10 and the start of the reference clock 20. PN0 sequence 12 has a period of PN0\_PRD and PN1 sequence 14 has a period of PN1\_PRD. One period of the augmented PN sequence 10 is formed from a first segment of PN0 sequence 12 defined by words 0 through INS\_IDX0-1 of the PN0 sequence 12, followed by a segment of from PN1 sequence (defined by a segment of SEG\_LTH words starting at position BEGIN\_IDX1 of the PN1 sequence 14), followed by a second segment of PN0 sequence 12 defined by words from position INS\_IDX0 to PN0\_PRD-1 of the PN0 sequence 12 (i.e., the remaining words of the PN0 sequence 12). Relative to the augmented PN sequence 10, the inserted segment is located in the sequence starting at position INS\_POS and ending on RET\_POS-1.

The output of the augmented PN sequence 10 can begin at any position in the augmented PN sequence 10. In the illustrated embodiment, the output of the augmented PN sequence 10 starts at the position labeled START.

Figure 3 illustrates a schematic representation of a circuit 30 which performs the function described hereinabove. The reference clock signal (REF\_CT) is input to one input of a subtractor circuit 32 along with the OFFSET signal. The output of the subtractor circuit 32 is input to a modulo circuit 33 which calculates the remainder of a division of the output of subtractor circuit 32 by AUG\_PRD. This remainder is coupled to the first input of dual port

multiplexer 34 and to a first input to subtractor 36. The second input to subtractor 36 is the segment length (SEG\_LTH), which is a constant during a given period of the augmented PN sequence (although it can change in subsequent periods). The output of subtractor 36 is coupled to the second input 5 to multiplexer 34. The output of multiplexer 34 coupled to a modulo circuit 35 (generating the remainder resulting from a division of the output of the multiplexer 34 with PN0\_PRD) which calculates idx\_A, which specifies a current index in the PN0 sequence. This index is coupled to the transition matrix 37 which is used by the PN0 pseudo-noise sequence generator 38 (typically a LFSR 10 or similar circuit) to generate the PN0 sequence. An embodiment for the LFSR and transition matrix are discussed in greater detail in U.S. Ser. No. 09/222,454, entitled "State Calculation Circuit for Discrete Linear State Space Model" to Gu, assigned to TEXAS INSTRUMENTS INCORPORATED of Dallas, Texas, filed December 29, 1998, which is incorporated by reference herein.

15       REF\_CT is also coupled adder 40 along with the two's complement of INS\_POS and BEGIN\_IDX1(see Figure 2) to adder 40, which sums the three inputs. The output of adder 40 is coupled to a first input of multiplexer 42 and to an input of adder 44. The second input of adder 42 is coupled to AUG\_PRD (see Figure 2). The output of adder 44 is coupled to a second input of multiplexer 42. 20 The output of multiplexer 42 is coupled to modulo circuit 46 (generating the remainder resulting from a division of the output of the multiplexer 42 with PN1\_PRD). The output of modulo circuit 46 is idx\_B, which specifies a current position in the PN1 sequence. This index is coupled to transition matrix 48 which is used by the PN1 pseudo-noise sequence generator 50 to generate the 25 PN1 sequence. The outputs of PN sequence generators 38 and 50 are coupled to inputs of dual port multiplexer 51. The multiplexer 51 selects between the two PN sequences to generate the augmented PN sequence.

A bank of comparators 52-57 perform various comparisons used to control multiplexers 34 and 42, PN sequence generators 38 and 50 and multiplexer 51.

Comparator 52 determines whether REF\_CT is equal to INS\_POS. Comparator 53 determines whether REF\_CT is equal to RET\_POS. Comparator 54 determines whether INS\_POS is greater than RET\_POS. Comparator 55 determines whether RET\_POS is greater than REF\_CT. Comparator 56 determines whether REF\_CT is greater or equal to INS\_POS. Comparator 57 determines whether REF\_CT is greater or equal to (INS\_POS -INS\_IDX0) mod AUG\_PRD. The outputs of comparators 54 and 55 are input to AND gate 58 to control multiplexer 42.

START is coupled first input gates in OR gates 60 and 62. The output of comparator 52 is coupled to the second input of OR gate 60 and the output of comparator 53 is coupled to the second input of OR gate 62. The output of OR gate 60 is coupled to a first input of AND gate 64 and the output of OR gate 62 is coupled to a first input of AND gate 66. The output of AND gate 64 is coupled to 15 a control port on PN1 sequence generator 50 and the output of AND gate 66 is coupled to a control port on PN0 sequence generator 38. The control ports on sequence generators 38 and 50 load the correct PN states from transition matrices 37 and 48, respectively, and thus reset the sequence generators to a predetermined point in the respective sequence for each period of the 20 augmented PN sequence.

The output of comparator 54 is also coupled to an inverted input of AND gate 68 and to a non-inverted input of AND gate 70. The output of comparator 55 is coupled to an input of AND gate 68 and to an input of OR gate 72. The output of comparator 56 is coupled to an input of AND gate 68 and to an input of 25 OR gate 72. The output of OR gate 72 is coupled to an input of AND gate 70. The outputs of AND gates 68 and 70 are coupled to inputs of OR gate 74. The output of OR gate 74 is the SEQ\_SEL signal which controls multiplexer 51 to select which sequence, PN0 or PN1, is output as the augmented PN sequence.

The output of OR gate 74 is also coupled to the inputs of And gates 64 and 66 to make sure that only one of the two PN generators is selected at a given time.

The output of comparator 56 is also output to OR gate 76 through an inverted input and to AND gate 78 through an inverted input. The output of 5 comparator 57 is coupled to a non-inverted input of OR gate 76 and to a non-inverted input of AND gate 78. Subtractor 80 receives INS\_POS and INS\_IDX0 (see Figure 2) and outputs the difference (INS\_POS -INS\_IDX0) to modulo circuit 82, which calculates (INS\_POS -INS\_IDX0) mod AUG\_PRD. The output of 10 modulo circuit 82 is coupled to the "B" input of comparator 57 and the sign bit of the difference calculation of subtractor 80 is coupled to an inverted input of AND gate 78 and to a non-inverted input of AND gate 84. The output of OR gate 76 is also coupled to an input of AND gate 84. The outputs of AND gates 78 and 84 are coupled to the inputs of OR gate 86. The output of OR gate 86 is the SEL0 signal which controls multiplexer 34.

15 In operation, the circuit works as follows. The SEQ\_SEL signal output from OR gate 74 switches between the outputs of the PN0 sequence generator 38 and the PN1 sequence generator 50. The PN0 sequence is effectively paused while the PN1 segment is inserted into the augmented PN sequence. Switching between the PN0 and PN1 sequences can be accomplished either by pausing the 20 generation of the PN0 or PN1 sequence when it is not selected by multiplexer 51 or by loading the sequence generators at appropriate times to start the sequence at a predetermined point. At steady state, the LOAD0 output from AND gate 66 starts the PN0 sequence at INS\_IDX0 after the PN1 segment is complete. The LOAD1 output from AND gate 64 starts the PN1 segment at the BEGIN\_IDX1 25 position when the augmented PN sequence has reached INS\_POS.

At the initial time, the START signal together with the other control signals decide the first bit of the augmented PN sequence 10 for output, since the

00000000000000000000000000000000

output can begin at any position within the PN0 sequence 12 or segment 16. The SEL0 signal (the output of OR gate 86) and the SEL1 signal (the output of AND gate 58), control the multiplexers 34 and 42 to select the correct PN index for T0 and T1, respectively, based on all of the input parameters. The SEL0 signal

5 provides for subtraction of SEG\_LTH from the output of the modulo circuit 33 after insertion of segment 16. The SEL1 signal accommodates the situation where the segment 16 spans the first bit of the augmented PN sequence 10, i.e., where INS\_POS precedes the first bit of the augmented PN sequence 10 and the RET\_POS is after the first bit of the augmented PN sequence 10.

10 Figure 4 illustrates a timing diagram where the PN0 sequence is augmented by segments from PN1 and PN2. In this case, the segment from PN1 is inserted at INS\_POS1 and the segment from PN2 is inserted at INS\_POS2. Any number of PN sequences could be used to generate the augmented PN sequence. Further, the segments could be inserted into other segments; for  
15 example, the PN2 sequence segment could be inserted into the PN1 segment.

Figure 5 illustrates a block diagram showing the use of the augmented PN sequence to encrypt a data stream. The pseudo-noise sequence generator 30 outputs a sequence of pseudo-noise words PN(k) to scrambler 90 along with data stream D(k). Data stream D(k) could be any digital data stream which would benefit from scrambling techniques, such as a digital communication signal or a native digital signal such as the output of a computing device. In the preferred embodiment, the scrambler circuit 90 performs an exclusive-or operation on the digital data stream D(k) and the pseudo-noise sequence PN(k) to generate the output S.

25 The present invention provides significant improvements over the prior art. Insertion of a one or more segments of arbitrary length at respective

arbitrary points in a PN sequence creates a PN sequence which is almost impossible to decipher.

Although the Detailed Description of the invention has been directed to certain exemplary embodiments, various modifications of these embodiments, as well as alternative embodiments, will be suggested to those skilled in the art. The invention encompasses any modifications or alternative embodiments that fall within the scope of the Claims.

## CLAIMS

1. A method of encrypting a digital signal comprising:  
2 generating a plurality of pseudo-noise sequences;  
4 combining said pseudo-noise sequences, or portions thereof, to generate  
an augmented pseudo-noise sequence; and  
4 encrypting a data stream using the augmented pseudo-noise sequence.

2. The method of claim 1 wherein said generating step comprises the  
2 step of generating first and second pseudo-noise sequences.

3. The method of claim 1 wherein said generating step comprises the  
2 step of generating three or more pseudo-noise sequences.

4. The method of claim 1 wherein said combining step comprises the  
2 step of inserting a segment of a first pseudo-noise sequence into a second  
4 pseudo-noise sequence at an arbitrary position in said second pseudo-noise  
sequence.

5. The method of claim 4 wherein said segment has an arbitrary  
2 length.

6. The method of claim 4 wherein said segment has arbitrary starting  
2 and ending positions within said first pseudo-noise sequence.

7. The method of claim 1 and further comprising the step of starting  
2 the output of the augmented pseudo-noise sequence at an arbitrary position in  
the sequence.

8. The method of claim 1 and further comprising the step of  
2 synchronizing the augmented pseudo-noise sequence to a reference clock.

9. The method of claim 8 wherein said synchronizing step comprises  
2 the step of synchronizing the augmented pseudo-noise sequence to a reference  
clock relative to an arbitrary offset.

✓ 10. Apparatus for encrypting a digital signal comprising:  
2 two or more pseudo-noise sequence generators  
4 circuitry for combining said pseudo-noise sequences, or portions thereof,  
to generate an augmented pseudo-noise sequence; and  
6 an encrypting circuit for correlating the augmented pseudo-noise  
sequence with a data stream.

11. The apparatus of claim 10 wherein said generating step comprises  
2 the step of generating first and second pseudo-noise sequences.

12. The apparatus of claim 10 wherein said two or more pseudo-noise  
2 sequence generators comprises three or more pseudo-noise sequence generators.

13. The apparatus of claim 10 wherein said combining circuitry  
2 comprises circuitry for inserting a segment of a first pseudo-noise sequence into  
a second pseudo-noise sequence at an arbitrary position in said second pseudo-  
4 noise sequence.

14. The apparatus of claim 13 wherein said segment has an arbitrary  
2 length.

15. The apparatus of claim 13 wherein said segment has arbitrary  
2 starting and ending positions within said first pseudo-noise sequence.

16. The apparatus of claim 13 wherein said encrypting circuit performs  
2 an exclusive-or operation.

17. The apparatus of claim 10 and further comprising circuitry for  
2 starting the output of the augmented pseudo-noise sequence at an arbitrary  
position in the sequence.

18. The apparatus of claim 10 and further comprising circuitry for  
2 synchronizing the augmented pseudo-noise sequence to a reference clock.

19. The apparatus of claim 18 wherein said synchronizing circuitry  
2 comprises circuitry for synchronizing the augmented pseudo-noise sequence to a  
reference clock relative to an arbitrary offset.

## ABSTRACT OF THE DISCLOSURE

An augmented pseudo-noise sequence (10) is generated from a two or more pseudo-noise sequences, using LFSRs or other such devices. A segment (16) of a one pseudo-noise sequence (14), having an arbitrary length, is inserted 5 into another pseudo-noise sequence (12) at an arbitrary position, making the augmented sequence difficult to decipher by a third party. Additional segments of arbitrary length can also be inserted at arbitrary positions for further complexity.

DNA Sequence

The diagram shows a horizontal line representing a DNA sequence. At the top left, there is a bracket labeled "DNA\_PRD". On the right side, there is a bracket labeled "14" above a wavy line and another bracket labeled "DNA\_PRD" below it. A vertical arrow points downwards from the top of the line to a point labeled "10". From this point, two arrows branch out: one pointing left labeled "SEA\_LTH" and one pointing right labeled "RET\_POS". Below the line, there is a bracket labeled "INS\_POS" with an arrow pointing to it. At the bottom left, there is a bracket labeled "PNT" with an arrow pointing to it. At the bottom right, there is a bracket labeled "12 PNT\_PRD" with an arrow pointing to it.

Augmented RN Sequence

$$AVG\_PRD = PNT\_PRD + SEQ\_LTH$$

RN Sequence

The diagram shows a horizontal line representing an RNA sequence. At the top left, there is a bracket labeled "PNT". On the right side, there is a bracket labeled "14" above a wavy line and another bracket labeled "PNT\_PRD" below it. A vertical arrow points downwards from the top of the line to a point labeled "10". From this point, two arrows branch out: one pointing left labeled "SEA\_LTH" and one pointing right labeled "RET\_POS". Below the line, there is a bracket labeled "INS\_POS" with an arrow pointing to it. At the bottom left, there is a bracket labeled "PNT" with an arrow pointing to it. At the bottom right, there is a bracket labeled "12 PNT\_PRD" with an arrow pointing to it.

FIG 1

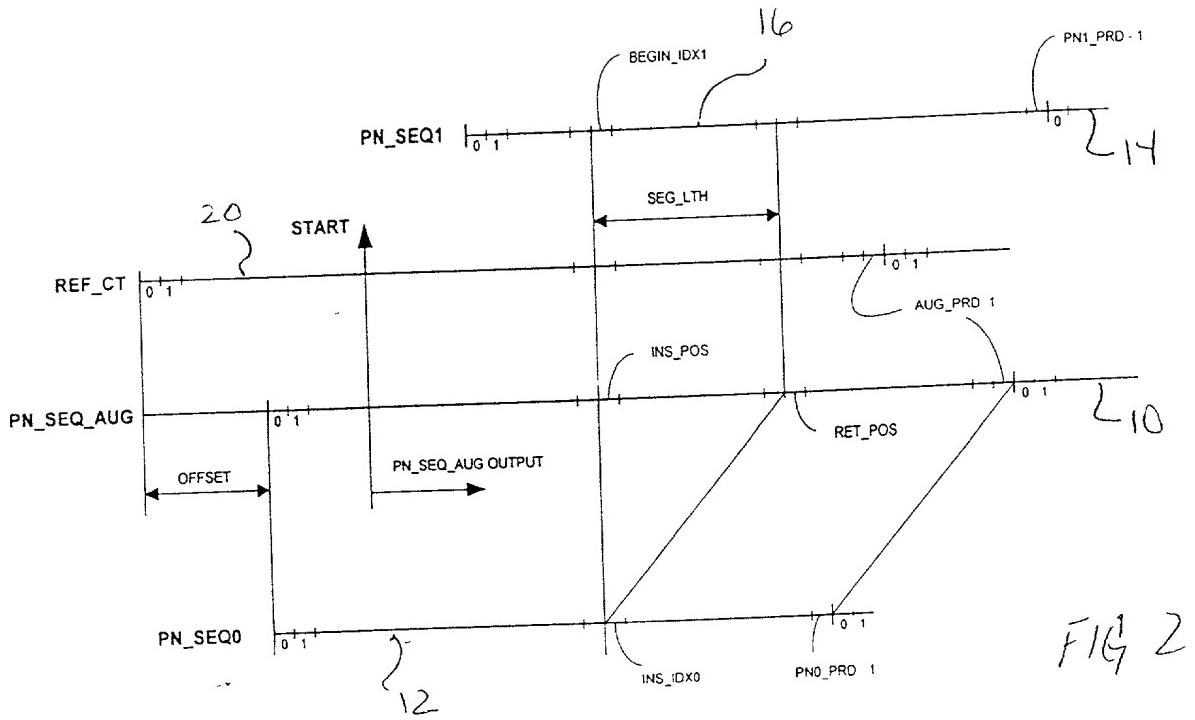


FIG 2

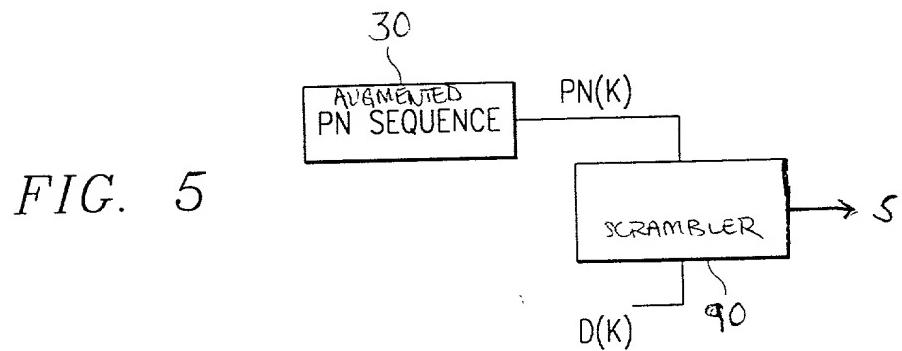


FIG. 5

30  
4

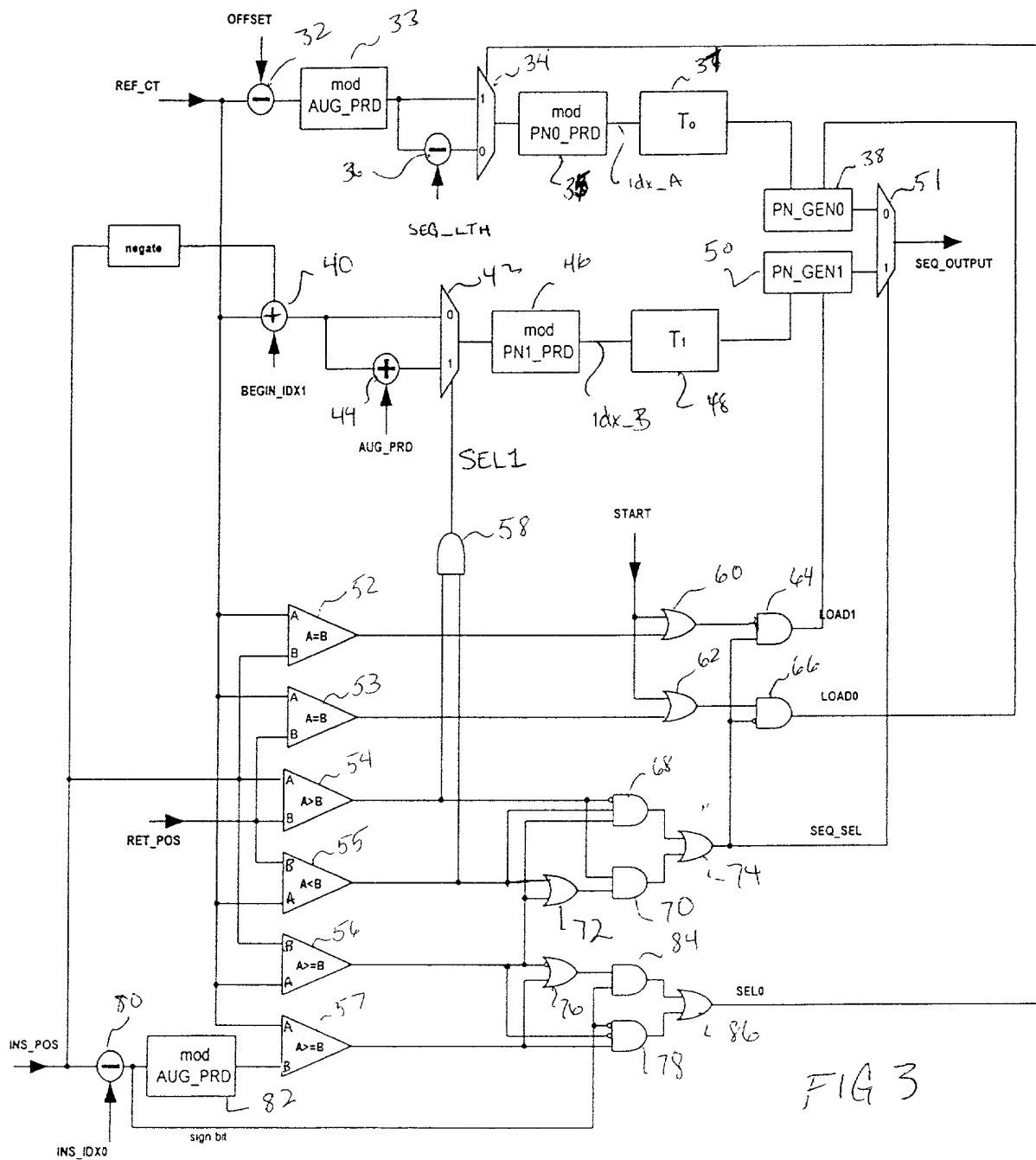


FIG 3

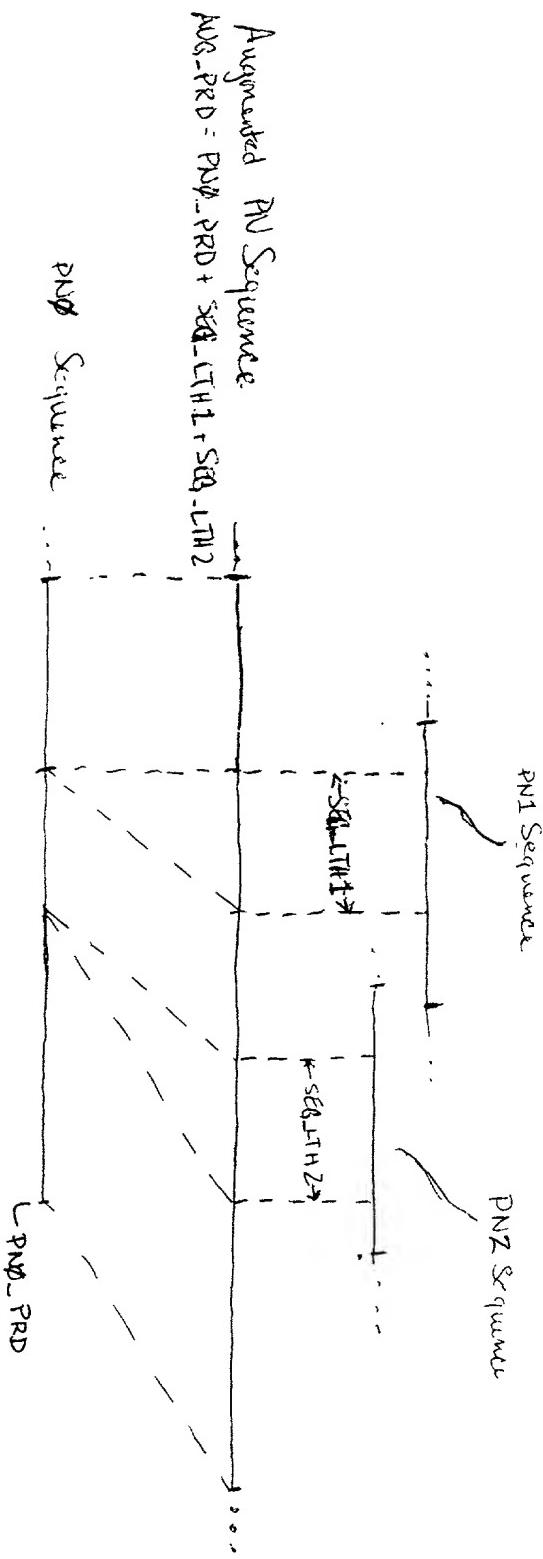


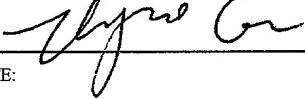
FIG 4

ATTORNEY'S DOCKET NO.  
TI-28444

APPLICATION FOR UNITED STATES PATENT  
DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I declare that my residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am the original, first and sole inventor if only one name is listed below, or an original, first and joint inventor if plural inventors are named below, of the subject matter which is claimed and for which a patent is sought on the invention entitled as set forth below, which is described in the attached specification; that I have reviewed and understand the contents of the specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration; that no application for patent or inventor's certificate on this invention has been filed by me or my legal representatives or assigns in any country foreign to the United States of America; and that I acknowledge my duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, section 1.56;

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

<b>TITLE OF INVENTION:</b> <b>Pseudo-Noise Sequence With Insertion Having Variant Length and Position</b>		
POWER OF ATTORNEY:	I HEREBY APPOINT THE FOLLOWING ATTORNEYS TO PROSECUTE THIS APPLICATION AND TRANSACT ALL BUSINESS IN THE PATENT AND TRADEMARK OFFICE CONNECTED THEREWITH  Ronald O. Neerings, Reg. No. 34,227; William B. Kempler, Reg. No. 28,228; Jay Cantor, Reg. No. 19,906; Robby T. Holland, Reg. No. 33,304; and Richard L. Donaldson, Reg. No. 25,673.	
SEND CORRESPONDENCE TO: Ronald O. Neerings, Esq. Texas Instruments Incorporated P. O. Box 655474, MS 3999 Dallas, Texas 75265	DIRECT TELEPHONE CALLS TO: Ronald O. Neerings, Esq. Phone Number: (972) 917-5299 Fax Number: (972) 917-4418	
NAME OF INVENTOR: Zhengou Gu	NAME OF INVENTOR:	NAME OF INVENTOR:
RESIDENCE & POST OFFICE ADDRESS: 8300 Monica Circle Plano, Texas 75025	RESIDENCE & POST OFFICE ADDRESS:	RESIDENCE & POST OFFICE ADDRESS:
COUNTRY OF CITIZENSHIP: People's Republic of China	COUNTRY OF CITIZENSHIP:	COUNTRY OF CITIZENSHIP:
SIGNATURE OF INVENTOR: 	SIGNATURE OF INVENTOR:	SIGNATURE OF INVENTOR:
DATE: 4/30/99	DATE:	DATE: